View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Elsevier - Publisher Connector

UN PROBLÈME SUR LES NOMBRES PSEUDO-PREMIERS

PAR

A. ROTKIEWICZ
(*Varsovie*)

(Communicated by Prof. J. G. VAN DER CORPUT at the meeting of September 25, 1971)

Pendant le Congrès International des Mathématiciens à Stockholm en 1962 M. H. J. A. Duparc m'a posé la question si pour tout nombre premier p et tous les nombres naturels a et b non divisibles par p il existe une infinité des nombres composés n, tels que $p|n$ et $n|a^{n-1}-b^{n-1}$, en signalant qu'il sait démontrer qu'il est ainsi, sauf dans le cas où $a^{p-1}-b^{p-1}$ n'a qu'un seul diviseur premier primitif égal à p.

Les nombres composés n qui satisfont la relation $n|a^{n-1}-b^{n-1}$ pour tout a et b avec $(ab, n)=1$ sont nommés absolument pseudo-premiers.

Pour $p=2$ le problème semble très difficile et je ne sais pas s'il existe pour tout nombre naturel a une infinité de nombres naturels n tels que $2|n$ et $n|(a+2)^{n-1}-a^{n-1}$. Cette propriété est vraie pour $a<13$ (voir [6]), mais la démonstration qu'il est ainsi pour tout a me semble difficile. Or pour $p>3$ on a le théorème suivant:

THÉORÈME 1. *Pour tout nombre premier $p>3$ et tous les nombres naturels a et b qui ne sont pas divisibles par p il existe une infinité de nombres naturels n tels que*

$$p|n \text{ et } n|a^{n-1}-b^{n-1}. \tag{1}$$

DÉMONSTRATION. Sans diminuer la généralité nous pouvons supposer que $(a, b)=1$ et $a>b$. S'il existe un nombre composé n pour lequel on a les formules (1), il en existe une infinité. En effet, soit $n=pm$ un nombre composé pour lequel on a les formules (1). Vu que $p>3$ et $m>1$, on a $n-1>2$, $n-1\neq 6$ et, en vertu du théorème de Zsigmondy-Birkhoff-Vandiver (voir [2], [4], [7], [11]) le nombre $a^{n-1}-b^{n-1}$ a un diviseur premier primitif q. On sait que ce diviseur premier primitif satisfait $q=(n-1)k+1$ où $k>1$ (dans le cas $k=1$ on aurait $q=n$, une impossibilité!).

En outre on a $(n, q)=1$, car sinon le nombre premier q diviserait n, contraire à $q=(n-1)k+1>(n-1)k>n-1$ donc $q\geqq n$. En vertu de $nq-1=$ $=n(n-1)k+n-1$ on a $n-1|nq-1$ donc $n|a^{nq-1}-b^{nq-1}$; aussi $q|a^{n-1}-$ $-b^{n-1}|a^{nq-1}-b^{nq-1}$, par conséquent en vertu de $(n, q)=1$ on a $nq|a^{nq-1}-$ $-b^{nq-1}$ (cf. aussi [1]).

Pour tout nombre composé n qui satisfait les formules (1) il existe donc

un nombre composé $N=nq>n$ pour lequel $N|a^{N-1}-b^{N-1}$ et $p|N$, d'où il résulte qu'il existe une infinité de nombres composés n pour lesquels on a les formules (1). Pour démontrer le théorème 1 il nous reste donc à trouver, pour tout nombre premier $p>3$, un nombre composé n pour lequel on a les formules (1).

Soit donc $p>3$ et $(p, ab)=1$. D'après le théorème de Fermat on a $p|a^{p-1}-1$ et $p|b^{p-1}-1$, d'où $p|a^{p-1}-b^{p-1}$. Si $p^2|a^{p-1}-b^{p-1}$, alors, vu que $p-1|p^2-1$, on a aussi $p^2|a^{p^2-1}-b^{p^2-1}$ et il existe un nombre composé $n=p^2$ remplissant les formules (1). Or, si $p^2\nmid a^{p-1}-b^{p-1}$, il suffira de démontrer que le nombre $a^{p-1}-b^{p-1}$ a un diviseur premier primitif $q>p$, puisque alors $p-1|q-1$, $p-1|pq-1$ et $pq|a^{pq-1}-b^{pq-1}$.

Or, on sait que (voir [4], [11]), tout diviseur premier primitif du nombre $a^{p-1}-b^{p-1}$, où $p>3$ et $(a, b)=1$, $a>b$, divise le nombre

$$f_{p-1}(a, b)=\prod_{i|p-1}(a^i-b^i)^{\mu(p-1/i)},$$

où $\mu(n)$ est la fonction de Möbius. Un diviseur premier du nombre $f_{p-1}(a, b)$, où

$$p-1=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k},\ (p_1<p_2<\dots<p_k)$$

est aussi un diviseur primitif du nombre $a^{p-1}-b^{p-1}$, où bien il est égal à p_k. S'il est p_k, on a $p_k^2\nmid f_{p-1}(a, b)$ et $p_1^{\alpha_1}p_2^{\alpha_2}\dots p_{k-1}^{\alpha_{k-1}}\,|\,p_k-1$. Pour démontrer que dans le cas, où $p^2\nmid a^{p-1}-b^{p-1}$, le nombre $a^{p-1}-b^{p-1}$ a un diviseur premier primitif $>p$, il suffira donc de démontrer que

$$f_{p-1}(a, b)>pp_\varepsilon, \tag{2}$$

où

$$p_\varepsilon=\begin{cases}1 \text{ si } p_1^{\alpha_1}p_2^{\alpha_2}\dots p_{k-1}^{\alpha_{k-1}}\nmid p_k-1;\\ p_k \text{ si } p_1^{\alpha_1}p_2^{\alpha_2}\dots p_{k-1}^{\alpha_{k-1}}\,|\,p_k-1.\end{cases}$$

Les nombres $n=3.11.17$, $5.13.17$, $7.13.19$ étant absolument pseudo-premiers, il existe un nombre n remplissant les formules (1) pour $p=5$, 7, 11, 13, 17, 19, si l'on a respectivement $(ab, 5.13.17)=1$, $(ab, 7.13.19)=1$, $(ab, 11.3.17)=1$, $(ab, 13.7.19)=1$, $(ab, 17.5.13)=1$, $(ab, 19.7.13)=1$. Pour démontrer que le théorème 1 est vrai pour $3<p\leqq 19$, il reste à vérifier que l'inégalité (2) est vraie pour $3<p\leqq 19$ lorsque ces plus grands diviseurs communs sont >1, ce qui a lieu, puisque nous avons

$$f_4(a, b)=a^2+b^2>10 \text{ pour } (ab, 5.13.17)>1,$$

$$f_6(a, b)=a^2-ab+b^2>3.7 \text{ pour } (ab, 7.13.19)>1,$$

et en outre nous trouvons pour $(ab, 3.5.7.11.13.17.19)>1$ que

$$f_{10}(a, b)=\frac{a^5+b^5}{a+b}>5.11,\ f_{12}(a, b)=\frac{a^6+b^6}{a^2+b^2}>3.13,\ f_{16}(a, b)=a^8+b^8>2.17,$$

$$f_{18}(a, b)=\frac{a^9+b^9}{a^3+b^3}>3.19.$$

Soit maintenant p un nombre premier >19. Nous utiliserons (voir [2], [4] et la formule (14) du travail [7]) l'inégalité

$$f_n(a, b) > 2^{\varphi(n)-2^{k-1}}, \tag{3}$$

où k indique le nombre des facteurs premiers différents de n.

Vu que pour $2<n\neq 6$ on a $\frac{1}{2}\varphi(n)\geqq 2^{k-1}$, il résulte de (3) que

$$f_n(a, b) > 2^{\varphi(n)/2} \text{ pour } 2<n\neq 6. \tag{4}$$

Si p est un nombre premier impair et si l'on a en outre

$$18<p-1\leqq 90,\ p-1=p_1^{\alpha_1}\ldots p_k^{\alpha_k},$$

nous vérifions directement que

$$2^{\varphi(p-1)-2^{k-1}} > pp_\varepsilon$$

et, d'après (3), on a l'inégalité (2). L'inégalité $f_{p-1}(a, b)>(p-1)^2$ entraînant l'inégalité (2), d'après (4) il suffira de démontrer que

$$2^{\varphi(n)/4} > n \text{ pour } n>90. \tag{5}$$

Or, comme on sait, $\varphi(n)>\sqrt{n}/4$ pour $n=1, 2, \ldots$ (voir [8], p. 142). Donc $2^{\varphi(n)/4}>2^{\sqrt{n}/16}\geqq n$ pour $n\geqq 2^{16}=65536$. Comme $\varphi(n)>n/6$ pour $n<2.10^9$ (voir [10], lemme 4.2), on a $2^{\varphi(n)/4}>2^{n/24}>n$ pour $192\leqq n<2.10^9$. Si $91\leqq n<192$, alors, vu que $2.3.5.7>192$, le nombre n a au plus trois diviseurs premiers, $\varphi(n)\geqq n(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5})=4n/15$ et $2^{\varphi(n)/4}>2^{n/15}>n$ pour $n\geqslant 101$. Or, on vérifie directement que $2^{\varphi(n)/4}>n$ pour $90<n<101$. Ainsi l'inégalité (5) et aussi le théorème 1 se trouvent démontrés.

THÉORÈME 2. *Pour tout nombre premier p et tout nombre naturel a non divisible par p il existe une infinité de nombres naturels n, tels que*

$$n|a^{n-1}-1 \text{ et } p|n. \tag{6}$$

DÉMONSTRATION. Pour $p=2$ le théorème 2 résulte des théorèmes 3 et 4 du travail [5].

Pour $p>3$ le théorème 2 résulte du théorème 1.

Soit donc $p=3$. Comme dans le cas $p>3$ il suffira de trouver un nombre composé n pour lequel $n|a^{n-1}-1$ et $3|n>3$. Comme $(a, 3)=1$, on a $3|a^2-1$. Si $9|a^2-1$, on a $9|a^8-1$ et un nombre n, pour lequel on a les formules (6) existe. Si $9\nmid a^2-1$ nous distinguons les cas suivants:

$a^2-1=3A$, $(A, 3)=1$ et A a un facteur premier $q>3$; alors on a
$q|a^2-1$, $3|a^2-1$, $(q, 3)=1 \Rightarrow 3q|a^2-1 \Rightarrow 3q|a^{3q-1}-1$;

$a^2-1=2^\alpha.3$, (1) $\alpha=0 \Rightarrow a=2$ alors $n|2^{n-1}-1$ pour $n=3.11.17$
(2) $\alpha>1$ ($\alpha=1$ est impossible)
a) $a-1\equiv 0$ (3) $\Rightarrow a-1\equiv 0$ (6) $\Rightarrow 6|a^5-1$
b) $a-1\not\equiv 0$ (3) $\Rightarrow a-1=2$ ou $a-1=2^{\alpha-1}$

(on verifie directement que $a-1=2^{\alpha-t}$ $(t>1)$ est impossible) mais $a=3$ n'est pas possible en vertu de $(a, 3)=1$, donc $a-1=2^{\alpha-1}$, $a^2-1=2^{\alpha}.3$, donc $a=5$ et $n|5^{n-1}-1$ pour $n=3.11.17$.

REMARQUE. Une analyse plus détaillée des cas $p=2$ et $p=3$ non contenus dans le théorème 1 nous amène à la conclusion que la réponse au problème de M. H. J. A. Duparc est toujours positive sauf, peut-être, dans les cas suivants avec $a>b$:

$$p=2,\ b=a-2,\ \text{a impair} \geqq 15,$$
$$p=3,\ a=3.2^{\alpha}+1,\ b=3.2^{\alpha}-1,\ \alpha \text{ naturel} \equiv 2 \pmod 5.$$

COROLLAIRE 1. *Pour tous les nombres naturels a et b et pour tout nombre premier p il existe une infinité de nombres composés n tels que*

$$p|n \text{ et } n|a^n b-ab^n. \tag{7}$$

DÉMONSTRATION. Pour $p=2$ le corollaire 1 résulte tout de suite du théorème 1 du travail [5].

Pour $p=3$ il suffira de trouver un nombre composé $n>7$ pour lequel on a les formules (7). En effet, soit $n=3m$ un nombre composé pour lequel on a les formules (7). Vu que $n>7$ on a $n-1>6$ et, en vertu du théorème de Zsigmondy-Birkhoff-Vandiver le nombre $a^{n-1}-b^{n-1}$ a un diviseur premier q tel que $n-1|q-1$; aussi

$$q|a^{n-1}-b^{n-1}|a^{nq-1}-b^{nq-1}|a^{nq}b-ab^{nq},\ q>n,$$

donc $nq|a^{nq}b-ab^{nq}$, $nq>n$. On a $3|n$, $n|a^n b-ab^n$ pour $n=3.11.17$ et pour $p=3$ il existe une infinité de nombres n pour lesquels on a les formules (7).

Soit $p>3$. Si $(ab, p)=1$, il résulte du théorème 1 qu'il existe une infinité de nombres n tels que $p|n$, $n|a^{n-1}-b^{n-1}$, donc aussi tels que $p|n$ et $n|ab(a^{n-1}-b^{n-1})=a^n b-ab^n$. Soit maintenant $(ab, p)=p$. D'après la démonstration du lemme 2 du travail [5] il suffira de trouver un nombre pair pour lequel on a les formules (7). Si $(ab, p)=p$, on a $2p|ab$ ou bien $p|ab$ et $2\nmid ab$. Si $2p|ab$, alors un nombre n pair pour lequel on a les formules (7) est le nombre $n=ab$, et si $p|ab$, $2\nmid ab$, un tel nombre est le nombre $n=2ab$.

COROLLAIRE 2. *Pour tout nombre naturel a et tout nombre premier p il existe un infinité de nombres composés n tels que*

$$p|n \text{ et } n|a^n-a. \tag{8}$$

M. H. J. A. Duparc s'occupe dans le travail [3] des nombres composés n tels que $n|a^{n-1}-1$ (où a est un nombre naturel >1). Il donne un exemple effectif des nombres composés jouissant de cette propriété, notamment

$$n=\begin{cases}\dfrac{a^{2a}-1}{a^2-1} \text{ si } a \text{ est un nombre premier } >2;\\[2ex] \dfrac{a^a-1}{a-1} \text{ si } a \text{ est un nombre composé.}\end{cases}$$

Or, il se montre en outre que pour les nombres a et b arbitraires on peut donner une formule explicite pour un nombre composé n tel que $n|a^{n-1}-b^{n-1}$. On a notamment le théorème suivant:

THÉORÈME 3. *Soient a et b des nombres naturels avec $a>b$ et $(a, b)=1$; désignons par $\overline{ab}$ le produit de tous les diviseurs premiers du nombre ab qui entrent dans le développement en facteurs premiers du nombre ab aux puissances avec les exposants impairs; soit donc $\overline{ab}=1$ si ab est un carré.*

Posons:

$$\eta = \begin{cases} 1 \text{ si } \overline{ab} \equiv 1 \pmod 4 \\ 2 \text{ si } \overline{ab} \equiv 2, 3 \pmod 4). \end{cases}$$

Alors pour $n=\eta\overline{ab}.15^t$ $(t=2, 3, \ldots)$ et

$$m=f_n(a, b)=\prod_{i/n}(a^i-b^i)^{\mu(n/i)},$$

(où μ est la fonction de Möbius), on a $m|a^{m-1}-b^{m-1}$.

DÉMONSTRATION. Soit $n=\eta\overline{ab}15^t$. Si $t>1$ on a $n>20$ et en vertu du théorème de A. SCHINZEL (voir [9]) le nombre a^n-b^n a deux diviseurs premiers primitifs. Comme chacun d'eux divise le nombre $f_n(a, b)$ (voir [4], [11]), $f_n(a, b)$ est un nombre composé.

Soit $n=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$, où $p_1<p_2<\ldots<p_k$ (donc $p_k\geqq 5$). Comme on sait (voir [4] et [11]) un diviseur premier du nombre $f_n(a, b)$ est un diviseur premier primitif du nombre a^n-b^n de la forme nk_1+1 ou bien de la forme p_k; s'il est égal à p_k, on a

$$p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_{k-1}^{\alpha_k-1} \mid p_k-1.$$

On a $(f_n(a, b), \eta\overline{ab})=1$. En effet, considérons les deux cas suivants:

I. Si $(f_n(a, b), \overline{ab})=q>1$ on aurait en vertu de la definition de $f_n(a, b)$ la relation $(a, b)\geqq q>1$.

II. Supposons $2\nmid f_n(a, b)$ pour $n\neq 2^v$ $(v=0, 1, 2, \ldots)$ (voir [11]) (N.B. n est composé). Donc, s'il était $p_k|f_n(a, b)$ pour $n=\eta\overline{ab}\ 15^t$, on aurait $p_k=5$, ce qui est impossible, puisque $3\nmid 5-1$. Donc tout diviseur premier du nombre $f_n(a, b)$ pour $n=\eta\overline{ab}.15^t$ (où $t=2, 3, \ldots$), donc aussi le nombre $f_n(a, b)$ lui même, sont de la forme $nt+1$. Donc $n|f_n(a, b)-1$, d'où il résulte que $f_n(a, b)|a^n-b^n|a^{f_n(a,b)-1}-b^{f_n(a,b)-1}$, et le théorème 3 se trouve démontré.

Institut Mathématique,
Académie Polonaise des Sciences
Warszawa 1
ul. Śniadeckich 8, Pologne

OEUVRES CITÉS

1. BEEGER, N. G. W. H., On even numbers m dividing 2^m-2, American Math. Monthly **58**, 553–555 (1951).
2. BIRKHOFF, G. D. and H. S. VANDIVER, On the integral divisors of a^n-b^n, Annals of Math. (2) **5**, 173–180 (1904).
3. DUPARC, H. J. A., On almost primes, Mathemat. Centrum Amsterdam, Rapport Z.W. 1955–012.
4. KANOLD, H. J., Sätze über Kreisteilungspolynome und ihre Anwendungen auf einige zahlentheoretische Probleme, I, Journ. reine und angew. Math. **187**, 169–182 (1950).
5. ROTKIEWICZ, A., Sur les nombres pairs a pour lesquels les nombres a^nb-ab^n, respectivement $a^{n-1}-b^{n-1}$ sont divisibles par n, Rendiconti Circolo Mat. Palermo (2) **8**, 341–342 (1959).
6. ————, Sur les nombres pairs n qui divisent $(a+2)^{n-1}-a^{n-1}$, ibidem (2) **9**, 78–80 (1960).
7. ————, Elementarny dowód istnienia dzielnika pierwszgo pierwotnego liczby a^n-b^n, Prace Mat. **4**, 21–28 (1960).
8. SIERPIŃSKI, W., Teoria Liczb, Warszawa-Wrocław 1950.
9. SCHINZEL, A., On primitive prime factors of a^n-b^n, Proc. Cambridge Philos. Soc. **58**, 555–562 (1962).
10. WARD, M., The intrinsic divisors of Lehmer numbers, Annals of Math. (2) **62**, 230–236 (1955).
11. ZSIGMONDY, K., Zur Theorie der Potenzreste, Monatshefte Math. Phys. **3**, 265–284 (1892).